AMENDMENTS TO THE CLAIMS

1-15. (Canceled)

16. (New) A data processing device for playing back a digital work recorded on a recording medium having also recorded (i) a plurality of record digest values generated from a plurality of data blocks constituting the digital work and (ii) record signature data generated by applying, with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values, comprising:

a verification key storing unit storing a verification key corresponding to the signature key;

a using unit operable to play back the digital work;

a selecting unit operable to randomly select a predetermined number of data blocks from the plurality of data blocks;

a calculating unit operable to calculate a plurality of calculation digest values from the selected data blocks;

a reading unit operable to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values;

a generating unit operable to generate a second combination based on calculation digest values and the remaining record digest values, the second combination being the same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values;

a signature verifying unit operable to perform a signature verification by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data; and

a use controlling unit operable to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

17. (New) The data processing device of Claim 16, wherein

the plurality of record digest values include a plurality of primary record digest values, each of which is generated for one of the plurality of data blocks, and a plurality of secondary

record digest values generated from two or more of the plurality of primary record digest values, and the record signature data is generated by applying, with use of the signature key, the signature generating algorithm to the first combination made of some or all of the plurality of secondary record digest values,

the reading unit reads, from the recording medium, the plurality of secondary record digest values and the remaining record digest values from among the plurality of primary record digest values, and

the generating unit includes:

a calculating subunit operable to calculate one or more secondary calculation digest values based on the calculation digest values and the remaining record digest values; and

a combining subunit operable to generate the second combination based on the plurality of secondary record digest values and the one or more secondary calculation digest values, the second combination being the same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values.

18. (New) The data processing device of Claim 17, wherein

the digital work includes a plurality of files, each of which corresponds to one of the plurality of secondary record digest values and is constituted by two or more of the plurality of data blocks,

each of the plurality of secondary record digest values is generated by using primary record digest values corresponding one-to-one with the two or more of the plurality of data blocks constituting a file corresponding to the secondary record digest value,

the calculating subunit calculates a secondary calculation digest value, with respect to each file including at least one of the selected data blocks, by using primary record digest values corresponding to the unselected data blocks included in the file and the calculation digest value corresponding to the at least one of the selected data blocks,

the reading unit reads, with respect to each file including none of the selected data blocks, a secondary record digest value corresponding to the file, and

the combining subunit generates the second combination by combining the calculated secondary calculation digest values and the read secondary record digest values.

19. (New) The data processing device of Claim 18, wherein

the plurality of record digest values are hash values each generated by a hash function,

the calculating unit applies the hash function to each of the selected data blocks in order to calculate hash values which are the calculation digest values, and

the calculating subunit applies the hash function to the primary record digest values corresponding to the unselected data blocks and the calculation digest values in order to calculate hash values which are the secondary calculation digest values.

20. (New) The data processing device of Claim 18, comprising, instead of the use controlling unit:

a warning display unit operable to display, when the digital work is judged as not being valid, a notice of invalidity of the digital work.

21. (New) The data processing device of Claim 16 wherein the recording medium has additionally recorded (i) area information indicating an access permitted area, on the recording medium, that an external device is permitted to access and (ii) signature data generated by applying, with use of a signature key, the signature generating algorithm to part or all of the digital work and the area information, the data processing device further comprising:

an access prohibiting unit operable to prohibit access to areas other than the access permitted area based on the area information;

a second verifying unit operable to perform a signature verification by applying, with use of a verification key, a signature verification algorithm to the digital work, the area information, and the signature data; and

a second use controlling unit operable to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

22. (New) The data processing device of Claim 16, wherein

the selecting unit, the calculating unit, the reading unit and the signature verifying unit are

assembled together in a single large scale integration.

23. (New) The data processing device of Claim 16, wherein

the reading unit reads record digest values corresponding to the selected data blocks from the recording medium, and

the data processing device further comprising:

a digest value verifying unit operable to make a judgment whether the plurality of record digest values recorded on the recording medium match calculation digest values; and

a third use controlling unit operable to stop the using unit from playing back the digital work when the judgment is affirmative.

24. (New) A recording medium used with the data processing device of Claim 16,

(i) having recorded thereon:

a digital work;

a plurality of record digest values generated from a plurality of data blocks constituting the digital work; and

record signature data generated based on the plurality of record digest values, and

(ii) supplying to the data processing device the digital work, the plurality of record digest values, and the record signature data.

25. (New) A data processing method (i) applied to a data processing device including: a verification key storage unit storing a verification key corresponding to a signature key; a using unit; a selecting unit; a calculating unit; a reading unit; a generating unit; a signature verifying unit; and a user control unit, and reading a digital work from a recording medium having recorded thereon: the digital work; a plurality of record digest values generated from a plurality of data blocks constituting the digital work; record signature data generated by applying, with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values, the data processing method comprising:

a using step of causing the using unit to play back the digital work;

a selecting step of causing the selecting unit to randomly select a predetermined number of data blocks from the plurality of data blocks;

a calculating step of causing the calculating unit to calculate a plurality of calculation digest values from the selected data blocks;

a reading step of causing the reading unit to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values;

a generating step of causing the generating unit to generate a second combination based on calculation digest values and the remaining record digest values, the second combination being the same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values;

a signature verifying step of causing the signature verifying unit to perform a signature verification by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data; and

a use controlling step of causing the use controlling unit to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

26. (New) A data processing program (i) applied to a data processing device including: a verification key storage unit storing a verification key corresponding to a signature key; a using unit; a selecting unit; a calculating unit; a reading unit; a generating unit; a signature verifying unit; and a user control unit, and reading a digital work from a recording medium having recorded thereon: the digital work; a plurality of record digest values generated from a plurality of data blocks constituting the digital work; record signature data generated by applying, with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values, the data processing program causing the data processing device to execute:

a using step of causing the using unit to play back the digital work;

a selecting step of causing the selecting unit to randomly select a predetermined number of data blocks from the plurality of data blocks;

a calculating step of causing the calculating unit to calculate a plurality of calculation digest values from the selected data blocks;

a reading step of causing the reading unit to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values;

a generating step of causing the generating unit to generate a second combination based on calculation digest values and the remaining record digest values, the second combination being the same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values;

a signature verifying step of causing the signature verifying unit to perform a signature verification by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data; and

a use controlling step of causing the use controlling unit to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

27. (New) The data processing program of Claim 26 recorded on a computer-readable recording medium.